

جمهورية مصر العربية

وزارة الاتصالات والمعلومات

اسم الملف:

e-Government
Code of Practice for Information Security Management
v1.3

الغرض من الوثيقة:

تقديم معايير إدارة وتأمين المعلومات داخل القطاعات الحكومية

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون (202) 3088299
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg

المحتويات

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون 3088299 (202)
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون 3088299 (202)
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg

الغرض من الوثيقة

تقديم معيار التوصيات الخاصة بإدارة أمن المعلومات لاستخدام الأفراد المسئولين عن أمن تنفيذ أو صيانة المعلومات في المؤسسات التابعين لها، وذلك بهدف توفير قاعدة عامة لإعداد معايير الأمن المؤسسي وإدارة الأمن بفاعلية والثقة في التعاملات الداخلية بالمؤسسة.

يجب اختيار وتطبيق توصيات هذه المعايير وفقا للقوانين واللوائح السارية.

الموجز التنفيذي

ما هو تأمين المعلومات ؟

تعد المعلومات أصولاً ذات قيمة بالنسبة لهيئة ما، مثلها فى ذلك مثل الأصول الأخرى الخاصة بالأعمال، و بالتبعية فهى تحتاج لأن تتوافر لها الحماية المناسبة. إن تأمين المعلومات يوفرالحماية لهذه المعلومات من الكثير مما يهددها، و ذلك بهدف التأكد من إستمرارية العمل، و لتقليل إحتمالات الخسارة فى الأعمال و لرفع العائد للحد الأقصى على الإستثمارات و على فرص العمل.

تكون تلك المعلومات على هيئة أشكال متعددة. فمن الممكن أن تكون مطبوعة أو مكتوبة على الورق، أن يتم تخزينها الكترونياً، يتم نقلها عن طرق البريد أو باستخدام وسائل الكترونية، يمكن مشاهدة المعلومات فى أفلام، أو يتم تبادلها فى محادثة. فبغض النظر عن الشكل الذى تكون عليه المعلومات ، و الوسيلة التى يتم عن طريقها تخزين المعلومات أو تبادلها، يجب دائماً أن تتم حماية تلك المعلومات بطريقة مناسبة.

يوصف مبدأ تأمين المعلومات بأنه للمحافظة على :

أ) السرية : وذلك من خلال التأكد من أن المعلومات متاحة فقط لمن هم مصرح لهم بالوصول إليها،

ب) التكامل : و يتمثل فى حماية دقة المعلومات و تمامها و حماية طرق معالجتها،

ت) التوافر: التأكد من أن المستخدمين المصرح لهم يمكنهم الوصول إلى المعلومات و إلى الأصول المضمنة، وقت حاجتهم لها.

يتحقق تأمين المعلومات عن طريق تشغيل مجموعة مناسبة من أنظمة التحكم ، قد تكون سياسات، ممارسات، إجراءات، هياكل مؤسسية أو وظائف برمجيات. يجب أن يتم وضع تلك الأنظمة للتأكد من أن أهداف التأمين الخاصة بكل هيئة قد تم بالفعل تحقيقها.

تليفون 3088299 (202)
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg
برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية

ماهى الحاجة لتأمين المعلومات ؟

تعد كل من المعلومات ، عمليات الدعم، الأنظمة و الشبكات ذات أهمية لأصول الأعمال. قد تكون السرية، التكامل و توافر المعلومات أساسية للحرص على الحد التنافسى، سيولة الأموال، مقدار المكسب، الإذعان للقانون، و الرؤية التجارية. و بشكل متزايد، تواجه الهيئات و أنظمة المعلومات و الشبكات الخاصة بها تهديدات أمنية عديدة من مصادر مختلفة، بما فيها الخداع بإستخدام الكمبيوتر، التجسس، التخريب، التخريب المتعمد، الحريق أو الغرق.
إن مصادر الضرر مثل الفيروسات التى تصيب أجهزة الكمبيوتر، إختراق أجهزة الكمبيوتر و محاولات الهجوم لرفض الخدمة، كل ذلك أصبح أكثر شيوعاً ، و بتطلع متزايد و بصورة تزداد تعقيداً يوماً بعد يوم.

إن تبعية أنظمة المعلومات و الخدمات يعنى أن الهيئات غير محصنة بالدرجة الكافية ضد محاولات تهديد تأمينها.
إن الإتصال الداخلى بين الشبكات الخاصة والعامة و تبادل مصادر المعلومات، كل ذلك يزيد من صعوبة تحقيق التحكم فى الوصول للمعلومات. إن الإتجاه لتوزيع الميكنة قد تسبب فى ضعف فاعلية نظام التحكم المركزى و المتخصص. لم يتم تصميم العديد من أنظمة المعلومات على أن يتم تأمينها. إن التأمين الذى يمكن تحقيقه من خلال الطرق التقنية يعد محدوداً، و يجب أن يتم تدعيمه من خلال إدارة و إجراءات مناسبة. إن تعريف ما هى نظم التحكم التى يجب توافرها يتطلب التخطيط الدقيق و الإنتباه للتفاصيل. تتطلب إدارة تأمين المعلومات، كحد أدنى، إشتراك كل العاملين فى الهيئة. قد تتطلب أيضاً مشاركة الموردين، العملاء و المساهمين. بالإضافة إلى ذلك ، قد تكون هناك حاجة لطلب إستشارة متخصصة من خارج الهيئات.
تعد أنظمة التحكم فى تأمين المعلومات منخفضة التكلفة بشكل ملحوظ وأكثر فاعلية إذا ما تم إدماجها فى مواصفات المتطلبات و مرحلة التصميم.

كيف يمكن تحديد متطلبات التأمين؟

من الضرورى أن تحدد الهيئة متطلبات التأمين الخاصة بها. هناك ثلاثة مصادر رئيسية.
ينشق المصدر الأول من تحديد حجم المخاطر التى قد تتعرض لها الهيئة. من خلال تحديد حجم الخطر، يتم تعريف مدى ما يهدد الأصول، القابلية للإصابة و إحتمال الحدوث يتم تقييمهما و يتم تقدير التأثير المتوقع.
أما عن المصدر الثانى فهو المتطلبات التشريعية، القانونية، التنظيمية و التعاقدية التى يتحتم على الهيئة، و شركائها التجاريون، و المتعاقدون معها و مقدمى الخدمات أن يستوفوها.
بالنسبة للمصدر الثالث هو مجموعة المبادئ الخاصة، الأهداف، المتطلبات الخاصة بمعالجة المعلومات التى قامت الهيئة بتطويرها لدعم عملياتها.

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون 3088299 (202)
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg

تعيين مدى أهمية مخاطر التأمين:

يتم تعريف متطلبات التأمين من خلال طريقة تعيين نمطي لمخاطر التأمين. يجب عمل موازنة لنفقات إحتياجات أنظمة التحكم مقابل الضرر الذى يلحق بالأعمال الذى غالباً ما قد ينتج عن الفشل فى التأمين. يمكن تطبيق تقنيات تعيين المخاطر على الهيئة بأكملها، أو على أجزاء فقط منها، و أيضاً على أنظمة المعلومات الشخصية، المكونات الخاصة بالنظام أو الخدمات حينما يكون ذلك قابلاً للتطبيق، حيث يكون ذلك واقعياً و مفيداً.
إن تعيين المخاطر هو إعتبار نمطى من:

أ) الضرر الذى قد تتعرض له الأعمال غالباً كنتيجة للفشل فى التأمين، مع الوضع فى الإعتبار التبعات المتوقع حدوثها من فقدان للسرية، التكامل و مدى إتاحة المعلومات و الأصول الأخرى،
ب) الإحتمال الأرجح الواقعى لمثل هذا الفشل الذى يحدث فى ضوء التهديدات السائدة و القابلية للإصابة،و أنظمة التحكم التى تعمل حالياً.

ينتج عن هذا التعيين المساعدة فى توجيه و تحديد إجراء الإدارة المناسب وأولويات مخاطر إدارة تأمين المعلومات،
و تشغيل أنظمة التحكم التى تم إختيارها للحماية ضد هذه المخاطر. قد تحتاج عملية تعيين المخاطر و إختيار أنظمة التحكم إلى إجراء عدة مرات لتغطية الأجزاء المختلفة من الهيئة أو أنظمة المعلومات الشخصية.

من الضرورى أن تتم مراجعات بشكل دوري لمخاطر التأمين و لأنظمة التحكم التى تم تشغيلها للأسباب الآتية:

أ) ملاحظة التغييرات فى متطلبات و أولويات العمل،
ب) الوضع فى الإعتبار التهديدات و إحتمالات الإصابة الجديدة،
ت) التأكد من أن أنظمة التحكم لا تزال فعالة و مناسبة.

يجب أن تجرى هذه المراجعات على مستويات من العمق مختلفة وفقاً لنتائج التعيينات السابقة و المستويات المتغيرة للمخاطر التى تكون الإدارة مستعدة لتقبلها.غالباً ما تكون تعيينات المخاطر فى المقام الأول، مما يعنى إعطاء الأولوية للمصادر فى المناطق العالية المخاطر، ثم للمستوى التفصيلى، لتوجيه المخاطر المحددة.

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابي
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون 3088299 (202)
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg

اختيار أنظمة التحكم:

طالما تم تعريف متطلبات التأمين، يمكن إختيار و تشغيل أنظمة التحكم للتأكد من تقليل من المخاطر للوصول بها لمستوى مقبول. يمكن إختيار انظمة التحكم من هذا الملف أو من مجموعات أنظمة التحكم الأخرى، أو من أنظمة التحكم الجديدة التى يمكن تصميمها لتناسب الإحتياجات الخاصة بطريقة مناسبة.

هناك العديد من الطرق لإدارة المخاطر ويوفر هذا الملف عدة أمثلة للإتجاهات المشتركة.

على أية حال، من الضرورى أن نعترف بأن بعض أنظمة التحكم ليست قابلة للتنفيذ لكل أنظمة و بيئات المعلومات، وقد تكون غير قابلة للممارسة فى جميع الهيئات. على سبيل المثال، فقرة 9.7 و 12.1 تصف كيفية مراقبة إستخدام نظام ما و كيفية جمع الدلائل. إن أنظمة التحكم المشروحة مثل الدخول إلى الحدث قد تحدث إشكالاً مع التشريع المعمول به، مثل حماية سرية العملاء أو فى مكان العمل.

يجب إختيار أنظمة التحكم على أساس تكلفة التنفيذ بالنسبة للمخاطر التى يمكن الإقلال منها و الخسائر المحتملة إذا حدث خرقاً لهذا التأمين. كما يجب أيضاً الأخذ فى الإعتبار العوامل غير المالية مثل فقد سمعة الجهة.

من الممكن إعتبار بعض أنظمة التحكم فى هذا الملف لمبادئ مرشدة (موجه) لإدارة تأمين المعلومات وتعد قابلة للتطبيق على معظم الهيئات. يوجد شرح واف لهذه المبادئ تحت عنوان " نقطة البداية لتأمين المعلومات".

نقطة البداية لتأمين المعلومات :

يمكن الوضع فىالإعتبارعدد من أنظمة التحكم بإعتبارها مبادئ مرشدة توفر نقطة بداية جيدة لتنفيذ نظام تأمين معلومات. فإما أن تكون على أساس المتطلبات التشريعية الأساسية أو أن تعتبر الممارسة العامة الأفضل لتأمين المعلومات.

تتضمن أنظمة التحكم التى تعتبر أساسية لهيئة ما من وجهة النظر التشريعية ما يلى:

أ) حماية البيانات و سرية المعلومات الشخصية،
ب) حماية السجلات المنظمة،
ت) حقوق الملكية الفكرية.

تتضمن أنظمة التحكم التى تعتبر الممارسة العامة الأفضل لتأمين المعلومات ما يلى:

أ) ملف سياسة تأمين المعلومات،
ب) تحديد المسئوليات الخاصة بتأمين المعلومات،
ت) تعلم مبدأ تأمين المعلومات و التدريب عليه،
ث) عمل تقارير عن الحوادث العارضة المتعلقة بالتأمين،

ج) إدارة إستمرارية العمل.
تنطبق أنظمة التحكم تلك على معظم الهيئات و فى ظل معظم بيئات المعلومات. من الجدير بالذكر أن بالرغم من أن معظم أنظمة التحكم فى هذا الملف تعد ذات أهمية، فإن تحديد ما إذا كان نظام التحكم وثيق الصلة بالموضوع يجب أن يكون فى ضوء المخاطر المحددة التى تواجهها الهيئة. و من هنا، فبالرغم من أن الإتجاه السابق ذكره يعتبر نقطة بداية جيدة، إلا أنه ليس بديلاً لإختيار انظمة التحكم التى تعتمد على تعيين المخاطر.

العوامل الحاسمة للنجاح:

أثبتت التجارب أن العوامل الآتية غالباً ما تكون حاسمة بادئ مرشدة توفر نقطة بداية جيدة لتنفيذ نظام تأمين لتنفيذ تأمين المعلومات بنجاح داخل هيئة ما:

أ) سياسة التأمين، الأهداف و الأنشطة التى تعكس أهداف العمل،
ب) طريقة لتنفيذ التأمين تكون متسقة مع الثقافة المنظمة،
ت) الدعم المرئى و الإلتزام من قبل الإدارة،
ث) الفهم الجيد لمتطلبات التأمين، تعيين و إدارة المخاطر،
ج) التسويق الفعال للتأمين على مستوى جميع العاملين و المديرين،
ح) توزيع التوجيه على سياسة تأمين المعلومات و المعايير على جيع العاملين و المقاولين،
خ) توفير التعليم و التدريب المناسب،
د) نظام قياس مفهوم ومتوازن يستخدم فى تقييم الآداء فى إدارة تأمين المعلومات و للتراحات الناتجة عن ذلك بغرض بالتحسين.

تطوير الخطوط العريضة الخاصة بك :

من الجائز إعتبار رمز الممارسة هذا كنقطة بداي لتطوير الدليل الخاص بكل منظمة. ليس كل دليل و نظام تحكم فى رمز الممارسة هذا يكون قابلا للتطبيق.
و أكثر من ذلك، قد تكون بعض أنظمة التحكم الإضافية غير المدرجة فى هذا الملف ضرورية و مطلوبة. و عندما يحدث ذلك، يكون من المفيد الإحتفاظ بمراجع متداخلة و التى تسهل من عمل الفحص التى يقوم بها المراجعين و الشركاء فى العمل.

برنامج الحكومة الإلكترونية
وزارة الاتصالات والمعلومات
1 شارع الحصرى متفرع من شارع أحمد عرابى
المهندسين الجيزة 12651 – جمهورية مصر العربية
تليفون (202) 3088299
موقع الانترنت http://www.mcit.gov.eg
بريد الكتروني egov@mcit.gov.eg